9-27-04 | TFW 2137

PATENT
Customer No. 22,852
Attorney Docket No. 7451.0003-02
InterTrust Ref. No.: IT-9.2 (US)

CERTIFICATE OF EXPRESS MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service's "Express Mail Post Office to Addressee" service under 37 CFR § 1.10, in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on September 23, 2004. Express Mail Label No.: EV527340655US

Signed: Athena E. Pretory

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	
Victor H. SHEAR et al.	Group Art Unit: 2137
Application No.: 09/925,072	Examiner: CALDWELL, Andrew T.
Filed: August 6, 2001	
For: SYSTEMS AND METHODS FOR USING CRYPTOGRAPHY TO PROTECT SECURE COMPUTING ENVIRONMENTS	Confirmation No.: 3373

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

NOTICE REGARDING RELATED OPPOSITION PROCEEDING IN AUSTRALIA

Applicants hereby notify the U.S. Patent and Trademark Office that one of the patents assigned to InterTrust Technologies Corporation ("InterTrust") and bearing relation to the instant application was involved in an Opposition proceeding in Australia. Applicants submit this paper and the associated Information Disclosure Statement in fulfillment of their duty to disclose information potentially material to patentability under 37 CFR §§1.56 and 1.97. This paper is being filed before the mailing date of a first Office Action on the merits for the above-referenced application.

The present application, Appln. No. 09/925,072, is a continuation of application No. 09/678,830 (now U.S. Patent No. 6,292,569), which is a continuation of application No. 08/689,754 (now U.S. Patent No. 6,157,721). The claims of the application opposed in Australia initially corresponded to the issued claims of U.S. Patent No. 6,157,721.

STATUS OF AUSTRALIAN OPPOSITION PROCEEDING

The status of the proceeding is as follows. On or about April 16, 2003 Microsoft Corporation served on InterTrust Technologies a Notice of Opposition under the Australian Patents Act of 1990 (Exhibit A). On July 16, 2003 Microsoft filed their Statement of Grounds and Particulars in Support of their Opposition (Exhibit B).

REMARKS

Applicants encourage the Examiner to carefully review the attached documents and let the Applicants know if any additional information is needed. As always, if the Examiner believes that any document referred to in these papers and not yet submitted may be helpful in resolving an issue before him and would like to review that or any other document, Applicants invite the Examiner to contact the undersigned at (650) 849-6643 so we may provide such document.

With this Notice, Applicants are also submitting an Information Disclosure Statement that includes copies of the references listed/described in the Australian

Opposition Proceeding papers attached hereto (i.e., Exhibits A and B). Applicants have reviewed voluminous documents to determine which references used by Microsoft in the Australian proceeding have not been cited in the pending application. References that have not already been cited to the Office are listed in the IDS form PTO-1449 filed contemporaneously with this Notice.

Applicants submit this Notice Regarding Related Opposition Proceeding in Australia in fulfillment of their duty to disclose information potentially material to patentability under 37 C.F.R. 1.56. This submission does not constitute an admission that any of the listed documents are material or constitute "prior art."

If there are any fees due with the filing of this Notice not already accounted for, please charge the fees to our Deposit Account No. 06-0916

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P.

Dated: September 23, 2004

By: _____
Andrew B. Schwaab
Reg. No. 38,611

Finnegan Henderson Farabow
Garrett & Dunner L.L.P.
1300 I Street, NW
Washington, D.C. 20005
(202) 408-4000
Customer No. 22,852

Section 59
Regulation 5.3

Australia
Patents Act 1990

NOTICE OF OPPOSITION

MICROSOFT CORPORATION of One Microsoft Way, Redmond, Washington, 98052-6399, United States of America, gives notice that it opposes the grant of a patent in respect of application number 57835 of 2001 (Serial number 756,500) in the name of INTERTRUST TECHNOLOGIES CORPORATION.

A copy of this notice was served on the applicant at its address for service on 16 April 2003.

The Opponent's address for service is:

Mallesons Stephen Jaques
Solicitors
Governor Phillip Tower
1 Farrer Place
SYDNEY NSW 2000
Telephone: (02) 9296 2000
Fax: (02) 9296 3999
Ref.: KAC:NM

DATED:

Microsoft Corporation
By its legal representative

Kim O'Connell
Mallesons Stephen Jaques

To: **THE COMMISSIONER OF PATENTS**
COMMONWEALTH OF AUSTRALIA

Fee: $550.00

17-4 opposition

Australia

Patents Act 1990

IN THE MATTER OF AUSTRALIAN PATENT APPLICATION NO. 57835 OF 2001 (SERIAL NUMBER 756500) in the name of INTERTRUST TECHNOLOGIES INC

and opposition thereto by

MICROSOFT CORPORATION

STATEMENT OF GROUNDS AND PARTICULARS IN SUPPORT OF OPPOSITION

We, Microsoft Corporation, of Redmond, Washington, United States of America (the "**Opponent**") provide the following information in support of the Notice of Opposition in relation to Patent Application No. 57835 of 2001 (serial number 756500).

Grounds of Opposition

The grounds of opposition are as follows:

Ground 1: Section 59(b)

That the invention is not a patentable invention because it does not comply with paragraph 18(1)(a) of the *Patents Act 1990* - it is not a manner of manufacture within the meaning of section 6 of the Statute of Monopolies.

Ground 2: Section 59(b)

That the invention is not a patentable invention because it does not comply with paragraph 18(1)(b)(i) of the *Patents Act 1990* - it is not novel.

Ground 3: Section 59(b)

That the invention is not a patentable invention because it does not comply with paragraph 18(1)(b)(ii) of the *Patents Act 1990* - it does not involve an inventive step.

Ground 4: Section 59(c)

That the invention is not a patentable invention because it does not comply with subsection 40(2) of the *Patents Act 1990* - it does not describe the invention fully, including the best method known to the Applicant of performing the invention.

Ground 5: Section 59(c)

That the invention is not a patentable invention because it does not comply with subsection 40(3) of the *Patents Act 1990* - the claims are not clear and succinct and fairly based on the matter described in the specification.

Particulars of Grounds

1 Manner of manufacture

1.1 The alleged invention claimed is not a manner of manufacture within the meaning of section 6 of the Statute of Monopolies in that it is simply the use of known computer hardware and known security algorithms to carry out a known method of doing business (software testing and electronic software distribution) for which the known properties of the hardware and security algorithms make them suitable. Additionally, the alleged invention claimed is merely an abstract idea, mathematical algorithm or business method *per se*. There is no technological improvement claimed by the Applicant.

1.2 The invention claimed is not a manner of manufacture within the meaning of section 6 of the Statute of Monopolies on the basis that it is "generally inconvenient" within the meaning of that section. A monopoly would be provided over a common and useful method of using a computer in a field of human endeavour, namely, business, where the conferral of monopoly rights is not required to encourage research into and development of such methods. The conferral of a monopoly in such circumstances would simply amount to a "windfall gain" to the Applicant.

1.3 The invention claimed is not a manner of manufacture within the meaning of section 6 of the Statute of Monopolies on the basis that it is "generally inconvenient" within the meaning of that section. A monopoly would be provided over useful methods of using a computer in a field of human endeavour, namely, to prevent electronic terrorism (as stated in the specification of the patent), where the conferral of monopoly rights would prevent research into and implementation of necessary computer security techniques contrary to the national interest.

2 Novelty

2.1 None of the claims of the Application are novel when compared with the prior art base as it existed before the priority date of each claim.

2.2 The prior art base for the purpose of paragraph 2.1 included:

(a) the following documents cited against the Application during its international phase and during the examination of the Application in Australia:

(i) US Pat. No. 4,930,073 (Cina, Jr.)

(ii) US Pat. No. 5,692,047 / AU 717,615 (McManis) [*See*, e.g., pp. 6, 8-13, 16-33 and Fig. 1].

(b) the following prior patent publications:

(i) US Pat. No. 5,757,915 / AU 65011/96 (Aucsmith)

(ii) WO 96/27155 / AU 711,733 (Ginter) [*See*, for example, pp. 242-245, 248-249, 423-433, 576-603, 655-663 and 872-877.]

(iii) US Pat. No. 5,253,297 / AU 653823 (Press).

(c) the following prior publications:

(i) Denning, D.E., "Cryptography and Data Security", 1982 ISBN 0-201-10150-5. [*See*, for example, sections 1.3, 3.6.1, 3.7, 4.1.3, 4.2, 4.3, 4.6, 5.2, 5.4, 5.5 and 5.6]

(ii) Department of Defense Standard, "Department of Defense Trusted Computer System Evaluation Criteria" DoD5200.28-STD, December 1985. [*See*, for example, paragraphs 3.3, 4.1, 4.2 and 6].

(iii) Everett, D., "Smart Card Tutorial" published in sections between September 1992 and September 1994 at http://www.smartcard.co.uk/resources/tutorials/. [*See*, for example, parts 2, 9-24 and 26.]

(iv) Fuchsberger, A., et al, "Public-key Cryptography on Smart Cards", Lecture Notes in Computer Science, 1995, pp. 250- 269 [*See*, e.g., pp. 265-266.]

(v) Gasser, G., et al, "The Digital Distributed System Security Architecture", 1989 [*See*, for example, pp. 1-5, 7-9 and 12.]

(vi) Herzberg, et al, "Public Protection of Software", ACM Transactions on Computer Systems, vol. 5, no. 4, Nov. 1987, pp. 371-393. [*See*, for example, pp.371-380 and 385-390.]

(vii) Press, J., "A New Approach to Cryptographic Facility Design", ICL Technical Journal, 8(3), May 1993, pp.492-505. [*All sections relevant*].

(viii) Rouaix, F., "A Web navigator with applets in Caml", 8 May 1996 [*All sections relevant*], and Rouaix, F., "MMM Documentation V 0.30 beta, undated [*See*, for example, section titled "Applets"], and Rouaix, F., "Caml Applets in MMM", undated [*See*, for example, section titled "Security Issues".]

(ix) Schneier, B., "Applied Cryptography", Second Edition, December 1995.[*See*, for example, pp. 47-74, 357-359, 367-368, 436-441, 466-474, 483-502 and 584-595.]

(x) Tardo, J. et al, "Mobile Agent Security and Telescript", COMPCON Spring '96 - 41st IEEE International Computer Conference, 25 to 28 February 1996 [*See*, for example, paragraphs 1.0, 2.0, 5.0 to 8.2 and 10.0.]

(xi) Tardo, J., "An Introduction to Safety and Security in Telescript", General Magic Inc., 1995 [*All sections relevant.*]

(xii) Tygar, D., et al, Dyad: A System for Using Physically Secure Coprocessors, CMU-CS-91-140R, Carnegie Mellon University, (4 May 1991) [*See*, for example, pp. 4-15 and 21-27.]

(xiii) Verisign Press Release, "Microsoft and Verisign Provide First Technology for Secure Downloading of Software over the Internet, 20 Software Vendors Lead Industry in Adopting Microsoft Authenticode" Technology, 7 August 1996 [*All pages relevant.*]

(xiv) Yee, B., Using Secure Coprocessors, CMU-CS-94-149, Carnegie Mellon University (1994) [*See*, for example, pp 1-3, 5, 7-10, 13-16, 19-22, 24, 31, 35-41, 71-73, 79 and all of chapter 5.]

(xv) Zimmerman, P., "Pretty Good Privacy: PGP User's Guide, revised 11 October 1994. [*See*, for example, Vol. 1, pp. 2, 4, 5, 7 ("Encrypting a Message to Multiple Recipients"), 10, 11, 14 and 16 and Vol. 2, pp. 3, 6, 7, 8 and 21-29.]

(d) the following prior uses:

(i) Microsoft Internet Explorer v3.0 beta, March 1996.

(ii) MMM Version 0.30 beta, 5 April 1996.

(iii) Caml Applets in MMM Version 0.30 beta, 5 April 1996.

(iv) Telescript, by General Magic, 1995.

(v) Authenticode with ActiveX, by Microsoft Corporation, 1996.

(vi) Inferno, by AT&T Bell Labs, 6 May 1996.

(vii) Perl, Penguin and Safe, at least as early as April 1996.

(viii) Tripwire, (as described in Kim, G.H., et al, Writing, Supporting, and Evaluating Tripwire: A Publicly Available Security Tool, Purdue Technical Report CSD-TR-91-019, 12 March 1991)

(ix) PGP, Version 2.6.2, 11 October 1994.

(x) Mondex Smart Card, 1995-1996.

(xi) Novell Netware. v3.11, v4.0.

3 Inventive Step

3.1 None of the claims of the Application involve an inventive step when compared with the prior art base as it existed before the priority date of each claim. The subject of each claim would have been obvious to a person skilled in the relevant art in the light of the common general knowledge as it existed in Australia before the priority date of each claim, such knowledge considered separately or together with prior art information a

person skilled in the relevant art would have ascertained, understood and regarded as relevant to work in the relevant art in Australia.

3.2 The Opponent will rely on the common general knowledge as it existed in Australia at or before the priority date of each claim, which includes, without limitation, the following knowledge:

(a) Computers are interconnected by networks, such as the Internet. Programs and data can be transferred between computers across networks.

(b) Devices, such as computers, can send and receive data and executable files, and execute executable files.

(c) Computer systems can distribute data and executable files over networks, including the Internet.

(d) Computer systems could use security features to protect the computer system from "hackers", Trojan horses and viruses.

(e) Portable computer languages, such as Java, allow computers to interactively and dynamically download executable files and computer program code fragments (sometimes called "applets") over an electronic network such as the Internet, and execute the downloaded executable files and code fragments locally.

(f) A common solution to the problem of user acceptance of downloadable executable content is to apply digital signatures.

(g) Digital signatures provide proof of integrity and, combined with digital certificates, can provide information on source and authorship.

(h) Senders can digitally sign material using public key cryptographic algorithms such as RSA or DSA. To this end, senders can generate key-pairs such that digital material encrypted with the "private key" (held only by the sender) can only be decrypted using the corresponding "public key" (which is distributed to all intended recipients). The resultant digital signature is then associated with the material that is the subject of the signature and distributed to recipients over untrusted media such as the Internet.

(i) Recipients of the digital material could verify the digital signature by decrypting the digital signature with the sender's public key. Since only the sender's private key could have encrypted the material such that the sender's public key could be used to decrypt the material, the recipient is able to verify the authenticity of the sender (i.e. to distinguish between trusted and untrusted files).

(j) Senders can apply a message digest algorithm such as MD5 or SHA-1 to the subject material prior to signing. By doing this, the sender is able to offer the recipient assurance that the signed material remained unchanged between being sent and received (commonly known as "integrity").

(k) Digital signature technology provides assurance in respect of attributes other than the authenticity of the sender or integrity. In particular, the use of digital

signatures can be combined with downloaded executable files and software testing techniques to provide the user of the receiving computer system assurance over an executable file's source, functionality and integrity.

(l) Devices can be classified based on various factors, including factors relating to security issues.

(m) Digital signatures can be used to designate a file for use by devices in a given security level.

(n) Operating systems often run code in a separate memory segment to prevent unauthorised access to resources.

(o) A processing environment can be configured to provide processing in an environment that will prevent code from maliciously or inadvertently accessing critical resources. Cryptographic algorithms and a memory to store cryptographic keys and algorithms can be used to provide such an environment.

(p) A processor could decide whether or not to execute a file, based on a number of circumstances or tests.

(q) A given cryptographic algorithm can be repeatedly applied to a given file using multiple keys, and multiple cryptographic algorithms can be applied to a given file using multiple keys (commonly known as 'multiple' and 'cascading' cryptographic operations, respectively).

(r) To decrease the probability of compromise, keeping secret (for example, in protected storage) the public values on which the certificates are based, thereby denying an attacker access to values that may aid in the attack..

(s) The use of digital signatures is combined with 'multiple' and 'cascading' cryptographic operations.

3.3 The common general knowledge for the purpose of paragraph 3.1 also included the following prior art information:

(a) the following documents cited against the Application during its international phase and during the examination of the Application in Australia:

(i) US Pat. No. 4,930,073 (Cina, Jr.)

(ii) US Pat. No. 5,692,047 / AU 717,615 (McManis) [*See*, e.g., pp. 6, 8-13, 16-33 and Fig. 1.]

(b) the following prior patent publications:

(i) US Pat. No. 5,757,915 / AU 65011/96 (Aucsmith)

(ii) WO 96/27155 / AU 711,733 (Ginter) [*See*, for example, pp. 242-245, 248-249, 423-433, 576-603, 655-663 and 872-877.]

(iii) US Pat. No. 5,218,605 (Low, et al).

(iv) US Pat. No. 5,253,297 / AU 653823 (Press).

(c) the following prior publications:

(i) Denning, D.E., "Cryptography and Data Security", 1982 ISBN 0-201-10150-5. [*See*, for example, sections 1.3, 3.6.1, 3.7, 4.1.3, 4.2, 4.3, 4.6, 5.2, 5.4, 5.5 and 5.6]

(ii) Department of Defense Standard, "Department of Defense Trusted Computer System Evaluation Criteria" DoD5200.28-STD, December 1985. [*See*, for example, paragraphs 3.3, 4.1, 4.2 and 6].

(iii) Everett, D., "Smart Card Tutorial" published in sections between September 1992 and September 1994 at http://www.smartcard.co.uk/resources/tutorials/. [*See*, for example, parts 2, 9-24 and 26.]

(iv) Fuchsberger, A., et al, "Public-key Cryptography on Smart Cards", Lecture Notes in Computer Science, 1995, pp. 250- 269 [*See*, e.g., pp. 265-266.]

(v) Gasser, G., et al, "The Digital Distributed System Security Architecture", 1989 [*See*, for example, pp. 1-5, 7-9 and 12.]

(vi) Herzberg, et al, "Public Protection of Software", ACM Transactions on Computer Systems, vol. 5, no. 4, Nov. 1987, pp. 371-393. [*See*, for example, pp.371-380 and 385-390.]

(vii) Press, J., "A New Approach to Cryptographic Facility Design", ICL Technical Journal, 8(3), May 1993, pp.492-505. [*All sections relevant*].

(viii) Rouaix, F., "A Web navigator with applets in Caml", 8 May 1996 [*All sections relevant*], and Rouaix, F., "MMM Documentation V 0.30 beta, undated [*See*, for example, section titled "Applets"], and Rouaix, F., "Caml Applets in MMM", undated [*See*, for example, section titled "Security Issues".]

(ix) Schneier, B., "Applied Cryptography", Second Edition, December 1995. [*See*, for example, pp. 47-74, 357-359, 367-368, 436-441, 466-474, 483-502 and 584-595.]

(x) Tardo, J. et al, "Mobile Agent Security and Telescript", COMPCON Spring '96 - 41st IEEE International Computer Conference, 25 to 28 February 1996 [*See*, for example, paragraphs 1.0, 2.0, 5.0 to 8.2 and 10.0.]

(xi) Tardo, J., "An Introduction to Safety and Security in Telescript", General Magic Inc., 1995 [*All sections relevant.*]

(xii) Tygar, D., et al, Dyad: A System for Using Physically Secure Coprocessors, CMU-CS-91-140R, Carnegie Mellon University, (4 May 1991) [*See*, for example, pp. 4-15 and 21-27.]

(xiii) Verisign Press Release, "Microsoft and Verisign Provide First Technology for Secure Downloading of Software over the Internet, 20 Software Vendors Lead Industry in Adopting Microsoft Authenticode" Technology, 7 August 1996 [*All pages relevant.*]

(xiv) Yee, B., Using Secure Coprocessors, CMU-CS-94-149, Carnegie Mellon University (1994) [*See,* for example, pp 1-3, 5, 7-10, 13-16, 19-22, 24, 31, 35-41, 71-73, 79 and all of chapter 5.]

(xv) Zimmerman, P., "Pretty Good Privacy: PGP User's Guide, revised 11 October 1994. [*See*, for example, Vol. 1, pp. 2, 4, 5, 7 ("Encrypting a Message to Multiple Recipients"), 10, 11, 14 and 16 and Vol. 2, pp. 3, 6, 7, 8 and 21-29.]

(xvi) Abadi, M., et al, "Authentication and Delegation with Smart-cards", 1992 [*See*, for example, pp. 1-6.]

(xvii) Beizer, B., "Software Testing Techniques", (Van Nostrand Reinhold) 1983 [*See*, for example, sections 1.3 and 7]

(xviii) Birrell, A., et al, "A Global Authentication Service without Global Trust", Proc. IEEE Symp on Security and Privacy, April 1986. [*See*, for example, pp. 1-8.]

(xix) Diffie, W., et al, "New Directions in Cryptography", IEEE Transactions on Information Theory 22 (6), pp. 644-654 (Nov. 1976). [*See*, for example, sections 3 and 4.]

(xx) Diffie, W., et al, "Authentication and Authenticated Key Exchanges", (1992 Kluwer Academic Publishers).

(xxi) Diffie, W., "The First Ten Years of Public Key Cryptography," Vol. 76, No. 5 (IEEE Proceedings, May 1988)

(xxii) Frederick, "Certification and Accreditation Approach", Proceedings of the 16th National Computer Security Conference, Sept. 20-23, 1993. [*See*, for example, pp. 266 and 270-71.]

(xxiii) Kim, G.H., et al, "The Design and Implementation of Tripwire: A File System Integrity Checker", Purdue Technical Report CSD-TR-93-071, November 19, 1993. [*See*, for example, pp. 1-6, Fig. 1, and paragraphs 4.4, 5.1 and 5.3

(xxiv) Kim, G.H., et al, "Writing, Supporting, and Evaluating Tripwire: A Publicly Available Security Tool", Purdue Technical Report CSD-TR-91-019, March 12, 1991. [*See*, for example, paragraphs 1.1, 1.2, 2.2, 3.1, 3.2, 3.3, and 4.1.]

(xxv) Kaner C., "Testing Computer Software", New York, van Nostrand Reinhold, 1993.

(xxvi) Lampson, B., "Protection", ACM Operating Systems Rev. 8, 1 (January 1974). [*See*, for example, pp. 2-9.]

(xxvii) Lampson, B., "Personal Distributed Computing: The Alto and Ethernet Software" 1988. [*See*, for example, section titled "Communication".]

(xxviii) Merkle, R., "Protocol for Public Key Cryptosystems", Proc. of IEEE Symp. on Security and Privacy, pp. 122—134, 1980. [*See*, for example, pp. 122-131].

(xxix) National Institute of Standards and Technology, "Capstone Chip Technology", Apr. 30 1993.

(xxx) Naccache, D., et al, "Cryptographic Smart Cards" IIEE Micro 16(3):14-24, June 1996. [*See*, for example, pp. 1-2, 5 and 9-11.]

(xxxi) Rivest, R., et al, "A Method for Obtaining Digital Signatures and Public-Key CryptoSystems", Communications of the ACM, 21(2), pp. 120-126 (Feb. 1978). [*See*, for example, pp. 1-6.]

(xxxii) Rozenblit, M., "Secure Software Distribution," 0-7803-1811- 0/94 IEEE (1994). [*See*, for example, pp. 486-496].

(xxxiii) Thompson, et al, "A Concept for Certification of an Army MLS Management Information System", Proceedings of the 16th National Computer Security Conference, Sept. 20-23, 1993 [*See*, for example, pp. 254-258.]

(xxxiv) Van Slype, "Natural Language Version of the Generic CITED model, Volume 1: Presentation of the generic model", 6 September 1993. [*See*, for example, paragraphs 2.1.4, 2.1.5, 2.2.2, 2.2.3, 2.2.4, 2.2.6, 2.3.2.2, 2.3.2.3 and 2.3.2.4].

(xxxv) Van Slype, "Natural Language Version of the Generic CITED model, Volume 2: CITED usage monitoring system design for computer based applications", 6 September 1993 [*See*, for example, paragraphs 2.1 and 2.3].

(xxxvi) Wiengart, "Physical Security for the uAbyss", IBM Thomas J. Watson Research Center, (1987) [*See*, for example, p. 52].

(xxxvii) Wobber, E., et al. "Authentication in the Taos Operating System", 10 December 1993 [*See*, for example, sections 1, 2, 3.2, 4.1, 4.2 and 4.3.]

(xxxviii) "X. 509 The Directory--Authentication Framework: Data Communications Network Directory, Recommendation X.509" (Melbourne, 14-25 November 1988) pp. 48-81.

(d) the following prior uses:

(i) Microsoft Internet Explorer v3.0 beta, March 1996.

(ii) MMM Version 0.30 beta, 5 April 1996.

(iii) Caml Applets in MMM Version 0.30 beta, 5 April 1996.

(iv) Telescript, by General Magic, 1995.

(v) Authenticode with ActiveX, by Microsoft Corporation, 1996.

(vi) Inferno, by AT&T Bell Labs, 6 May 1996.

(vii) Perl, Penguin and Safe, at least as early as April 1996.

(viii) Tripwire, (as described in Kim, G.H., et al, Writing, Supporting, and Evaluating Tripwire: A Publicly Available Security Tool, Purdue Technical Report CSD-TR-91-019, 12 March 1991)

(ix) PGP, Version 2.6.2, 11 October 1994.

(x) Mondex Smart Card, 1995-1996.

(xi) Novell Netware. v3.11, v4.0.

(xii) Cryptolope Containers, IBM Corporation, 1995-96

(e) the information stated to be prior art or background in the patent specification, including that information contained on pages 2 to 8 (line 20) and page 19 (line 5) to page 24 (line 7) of the patent specification; and

(f) the references cited to the U.S. Patent and Trademark Office in Information Disclosure Statements filed by the Applicant in relation to U.S. Patent Application Serial No. 08/689,754.

3.4 The Opponent will rely on the common general knowledge considered together with:

(a) any one item of prior art information referred to in paragraph 3.3 above; or

(b) a combination of any 2 or more pieces of prior art information referred to in paragraph 3.3 above, being information that a person skilled in the relevant art could be reasonably expected to have combined,

insofar as such prior art information does not form part of the common general knowledge.

4 Sufficiency

4.1 The specification is confusing and contradictory.

4.2 The specification does not describe essential features of the invention.

4.3 The specification depends for its sufficiency on references to other documents. The specification improperly relies on unpublished material not included in the specification.

4.4 The specification attempts to incorporate by reference unpublished material, referred to in the specification as "copending application Ser. No. 08/388,107", to describe essential features of the invention. It is unclear what "copending application Ser. No. 08/388,107" is a reference to.

4.5 The specification attempts to incorporate by reference unpublished material, referred to in the specification as "Ginter et. al.", to describe essential features of the invention. It is unclear what "Ginter et. al." is a reference to.

4.6 There is insufficient detail in the specification for a number of claimed elements, such as tamper resistant barriers, virtual distribution environment, load modules, protected processing environments, security levels, tamper resistant enclosure, tamper resistance, and secure execution spaces.

4.7 The specification does not describe in sufficient detail how the "distributing" steps of claim 1 are carried out (and there is consequent ambiguity in dependent claims 2, 3 and 4).

4.8 The specification does not describe in sufficient detail how the "distributing" steps of claims 10 and 30 are carried out.

4.9 The specification does not describe in sufficient detail how the step of "verifying that the load module satisfies the specification" (claim 5) is carried out.

4.10 The specification does not describe in sufficient detail how the step of "verifying that the executable satisfies the specification" (claim 25) is carried out.

4.11 The specification does not teach which analyzing tool(s) should be used to analyze and test load modules and determine if specifications are both accurate and complete, nor does the patent specification teach how to use such analyzing tool(s).

4.12 The specification provides insufficient detail regarding techniques for providing secure, tamper resistant execution spaces within a "protected processing environment" for computer programs and data.

4.13 The specification provides insufficient detail regarding techniques for securing "protected processing environments" against inauthentic "load modules" introduced by the computer owner, user, or any other party.

4.14 The specification provides insufficient details as to how a public key can be secured behind a tamper resistant barrier (for example, as recited in claim 26) or how a distributed verification public key is maintained within a tamper resistant enclosure (for example, as recited in claim 30).

4.15 The specification provides insufficient detail regarding secure key exchange protocols.

4.16 The specification does not teach how a "tamper resistant barrier" resists tampering.

4.17 Fig. 14 of the specification is unclear and is not described with sufficient detail, and accordingly, the invention is not described fully. For example, it is unclear (i) how the decision at block 509 is made, (ii) how the specifications are generated at block 514, (iii) how the verifying authority determines that it is desirable to make new specifications at block 510, (iv) how the appropriate digital signatures are selected at block 516, (v) how it is determined who the load module should be distributed to at block 518, (vi) how it is determined what should be distributed (e.g., load modules with digital signatures, digital signatures only, or digital signatures with associated descriptions, etc.) at block 518, and (vii) how the appropriate distribution techniques are selected and implemented at block 520.

5 Clear, succinct and fairly based

5.1 The use of the phrase "load module" in claims 1, 3 - 7, 9, 10, 12, 13, 14, 20 and 25 is not clear. The phrase is defined and used inconsistently within the specification.

5.2 The use of the phrase "security level" in claims 1, 10, 14, 18, 19, 21, 22, 30, 34, 38 and 39 is not clear. The phrase "security level" is not and cannot be quantified or measured objectively, and is thus vague, arbitrary, and subjective.

5.3 The use of the phrase "digitally signing a load module with a first digital signature" in claim 1 is unclear and ambiguous. One reading of this phrase is that the load module has a first digital signature in it. Another reading is that one digital signature is used to create another digital signature.

5.4 Claim 1 is unclear and is contrary to the specification. Additionally, the recited method in claim 1 does not produce a useful result. A digital signature of a load module is hashed data, and therefore cannot be executed. It is unclear whether a digital signature is distributed at all as a result of the claimed method. In the method of claim 1, it is unclear what is distributed at step (c) - is it the first load module as it existed prior to step (a) or the result of step (a)? If the former, then step (a) is irrelevant. If the latter, then the first load module cannot be used by the first device class.

5.5 In relation to claim 2, it is not clear who uses the digital signatures or where the digital signatures are used. If the digital signatures are used at the first and second device classes, it is unclear how the digital signatures were obtained by such device classes.

5.6 In relation to claim 3, it is not clear how the first load module and the first digital signature are both obtained by the first device class.

5.7 The use of the phrase, used in claims 1 and 21, of "a second device class having at least one of tamper resistance and security level different from the at least one of tamper resistance and security level of the first device class" is not clear.

5.8 The use of the phrase "tamper resistance" in claim 1, 2, 20, 21, 22 and 40 is not clear. The phrase "tamper resistance" is not or cannot be quantified or measured objectively, and is thus vague, arbitrary, and subjective.

5.9 In relation to the "distributing" steps in claim 1, it is unclear how the distribution takes place.

5.10 In relation to the "distributing" steps of claim 10, it is unclear how the distribution takes place and it is unclear on what basis and how the decision is made as to which keys are distributed to which environments. In relation to the "distributing" steps of claim 30, it is unclear how the distribution takes place and it is unclear on what basis and how the decision is made as to which keys are distributed to which execution spaces. One cannot determine from claim 10 and 30, or the specification, where a key will end up and how it will get there.

5.11 The use of the phrase "using the first and second digital signatures to prevent the tamper resistances or security levels of the first device from becoming equal" in claim 2 is not clear.

5.12 The use of the phrase "conditionally executing" in claims 3, 4, 23, 24 and 29 is not clear.

5.13 In relation to claim 5, it is uncertain to whom the digital certificate is issued. It is also uncertain how the step of "verifying that the load module satisfies the specification" is carried out.

5.14 The use of the term "specification" in claims 5, 13, 25 and 33 is unclear. The term is not defined meaningfully within the bounds of the patent specification nor is any example of a "specification" given.

5.15 The step, in claim 5, of "verifying that the load module satisfies the specification" is unclear and is not fairly based.

5.16 The use of the phrase "attesting to the results of the verifying step" in claims 5 and 25 is not clear and is not fairly based.

5.17 The use of the phrase "tamper resistant barrier" in claims 6, 9, 11, 14, 18, 26, 29, 34 and 38 is unclear. The phrase is not defined within the specification.

5.18 The use of the term "secure" and "secured" in claims 6, 9, 26, 29, 30 and 34 - 37 is not clear. A precise meaning cannot be derived from the specification. Additionally, the term is not and cannot be quantified or measured objectively, and is thus vague, arbitrary, and subjective.

5.19 In relation to claim 9, it is unclear how the results of step (c) determine the "executing" decision in step (d).

5.20 The use of the phrase "security level classification" in claims 10 and 30 is not clear. The phrase "security level classification" is not or cannot be quantified or measured objectively, and is thus vague, arbitrary, and subjective.

5.21 The use of the phrase "protected processing environment" in claims 10, 14 - 17 and 34 is not clear. The phrase is not defined within the specification.

5.22 The use of the phrase "virtual distribution environment" in claim 10 is not clear. The phrase is not defined within the specification.

5.23 The use of the phrase "same load module" in the claim 10 and 14 is not clear.

5.24 The use of the phrase "same software module" in claims 18 and 38 is not clear and is not fairly based. The phrase "software module" is not defined or used in the specification, nor can the meaning of "same" be ascertained.

5.25 Claim 19 is unclear, because it is self-referencing and is a dependent claim of itself.

5.26 In claim 20, in respect of the load module, it is unclear what aspect of the load module is being authenticated in steps (b) and (c).

5.27 The use of the phrase "subset" in claim 20 is not clear. Since "subset" may refer to the empty set, the claim requires nothing more than selecting two random digital signatures and "associating" them with a "load module".

5.28 The use of the term "associating" in claims 20 and 40 is not clear.

5.29 The use of the term "executable" in claims 21, 23 - 27, 29, 30, 32 - 34, 40 and 41 is not clear. The term is used inconsistently within the specification.

5.30 In relation to claim 25, it is uncertain to whom the digital certificate is issued. It is also uncertain as to how the step of "verifying that the executable satisfies the specification" is carried out.

5.31 The use of the phrase "same executable" claims 30 and 34 is not clear.

5.32 The use of the phrase "secure execution space" in claims 30 and 34 - 37 is not clear.

5.33 The use of the phrase "tamper resistant enclosure" in claim 31 is not clear. The phrase is not defined within the specification.

5.34 The use of the word "including" in claim 38 is not clear. It is not clear whether the single step recited in claim 38 is the only step of the method, or if other unstated steps are required.

5.35 The element "digital signature authenticating circuit" in claim 35 and claim 36 is unclear and not fairly based.

5.36 The term "different digital signature authenticating techniques" in claim 36 and claim 37 is unclear.

5.37 The phrase "web of trust" in claim 41 is unclear.

5.38 The use of the term "associated" in the claims is not clear.

5.39 Claims 1-13, 18-33 and 38-41 are unclear because it is uncertain who or what is carrying out the process claimed.

5.40 The claims relate to more than one concept and more than one process, and as such, cannot be sensibly understood in light of section 40(4) of the *Patents Act 1990*.

The Opponent's address for service is:

Mallesons Stephen Jaques
Level 60 Governor Phillip Tower
1 Farrer Place
Sydney NSW 2000

Dated this 16th day of July 2003

Neil Merry
.....
Kim O'Connell
Solicitor for the Opponent
by her employed solicitor